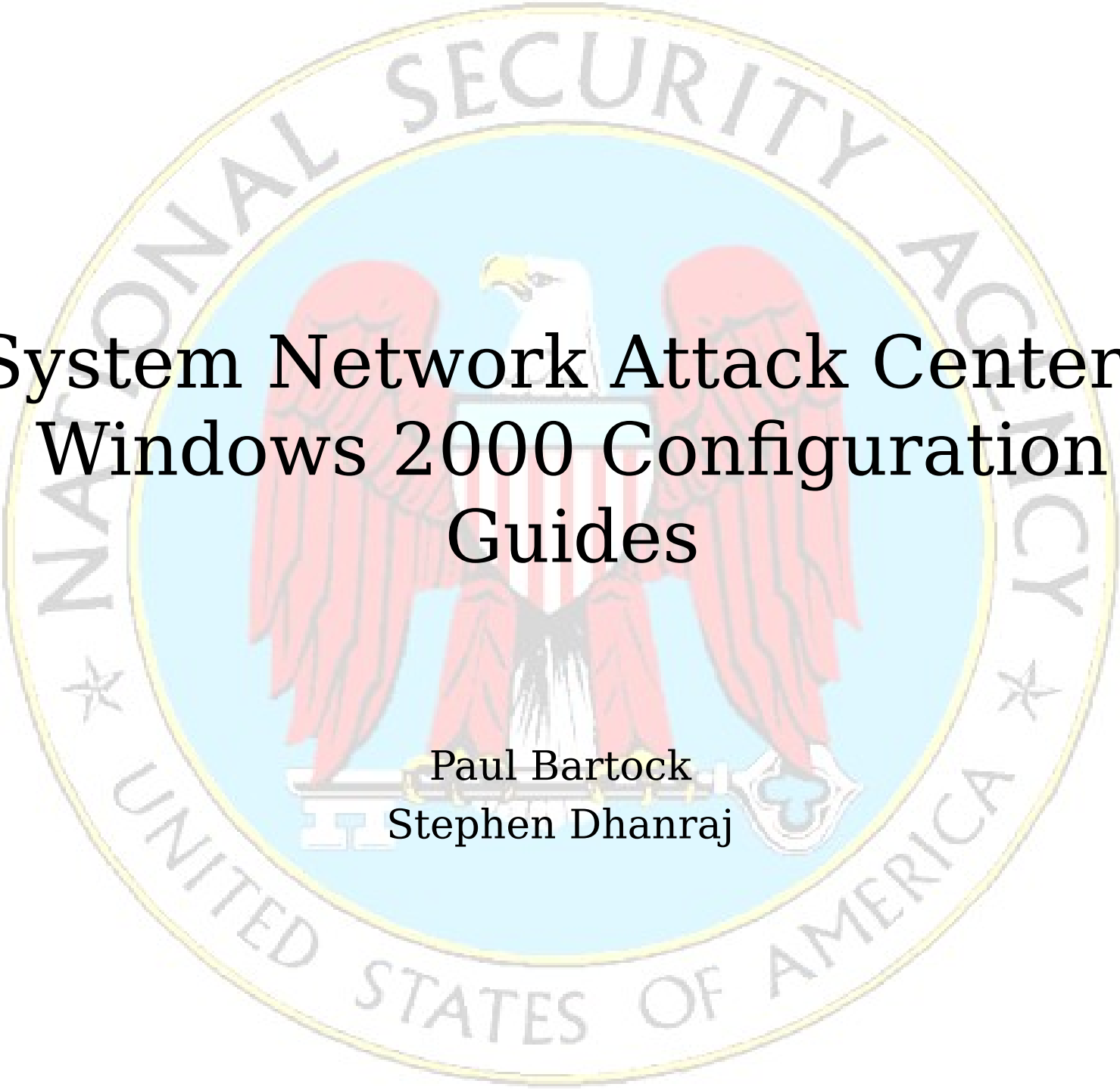




UNCLASSIFIED
D

The background of the slide features a large, faded seal of the National Security Agency. The seal is circular with a gold border. Inside the border, the words "NATIONAL SECURITY AGENCY" are written in a semi-circle at the top, and "UNITED STATES OF AMERICA" is written in a semi-circle at the bottom, separated by two stars. The center of the seal depicts an eagle with red wings and a white head, perched on a shield with vertical stripes. The eagle's talons are visible at the bottom.

System Network Attack Center Windows 2000 Configuration Guides

Paul Bartock
Stephen Dhanraj



Overview

- Background
- Windows 2000 Guide Development
- Who Expects the Guides
- Current Status

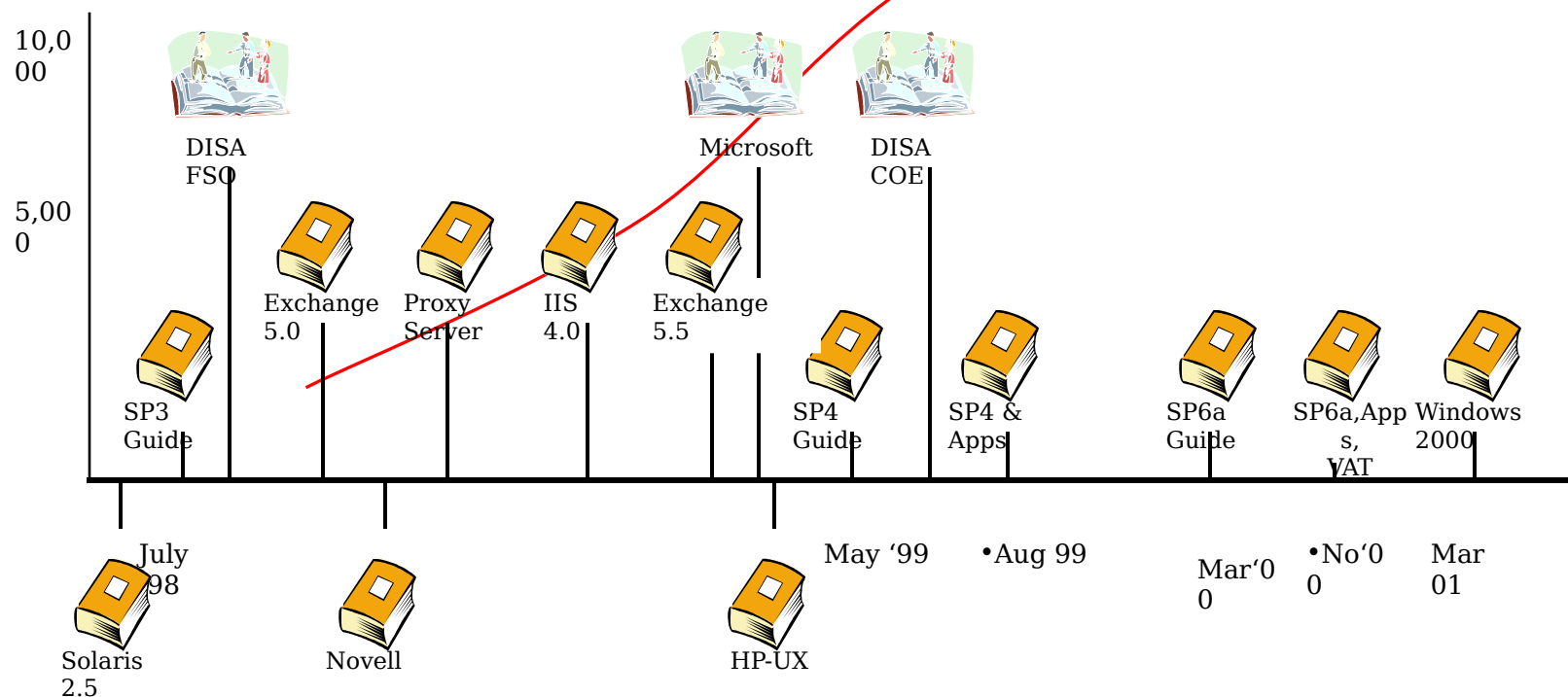


Background

- Created and distributed security configuration guides
 - Unix
 - Novell
 - Microsoft
- DoD entities expecting Win2K guide and offering resources



Background Guide Distribution Summary





Windows 2000 Guide Development Benefits

- Improve security of DoD systems and networks that incorporate Windows 2000
- Consolidate security configuration guidance throughout DoD and avoid conflicting and fragmented guidance
- Influence the way Microsoft baselines software releases for various customers
- Etc...



Windows 2000 Guide Development Windows 2000 Complexity

- **NT 4.0**
~ 483 security settings
2 man years
- **Windows 2000**
23 technologies
several thousands security settings
6 man years
baseline completion expected in eight months
(3/2001)



Windows 2000 Guide Development Process

- Develop mini-guides
 - Document and internal testing
 - Classification and tech writer reviews
 - Pre-Publication
 - Beta testing
 - Incorporate recommendations
- Develop Comprehensive Win2k guidance
 - combine mini-guides
- Release to customers



Windows 2000 Guide Development “mini-guides topics”

- Network Architecture
- Active Directory
- Group Policy
- IPSec
- Kerberos
- WINS
- Security Toolset
- Router and Firewall
- Non-Windows 2000 Clients
- NT to W2K Migration
- Mixed-mode
- Exchange 2000
- DNS



Windows 2000 Guide Development Who Is Offering Resources

- NSA
- DISA
- Mitre
- Microsoft Federal



Windows 2000 Guide Development Beta Testers (over 50)

- NSA
- DISA
- Microsoft
- SANS
- Mitre
- Air Force
- NIMA
- NASA (Houston , KSC, JPL)
- Department of STATE
- Social Security Administration
- IRS
- USDA
- OSD IPT committee
- DISA's NTAG committee



Who Expects Windows 2000 Guide

- DISA
- Navy – SPAWAR
- Marine Corp
- Department of Energy
- Department of State
- EUCOM
- TRANSCOM
- CENTOM
- Microsoft Federal
- CINCPAC
- AFIWC
- OSD
- Pentagon IT Infrastructure
- FDIC
- IRS
- EOP
- NSA NES Baseline
- Lockheed Martin



Current Status

- Started in October 2000
- 75 percent complete
- First release expected 6/2001



WINDOWS 2000 CONFIGURATION GUIDE STATUS (16 April 2001)

Topic	Priority	Guide Status	Projected Completion Date
1 - Network Architecture	High	Beta Testing	Dec-00
2 - Active Directory	High	Beta Testing	Mar-01
2a - Schema Customization	Low	Class review	Apr-01
3 - Group Policy	High		
3a - Software Settings	Med	Beta Testing	Feb-01
3b - Scripts	Med	Beta Testing	Mar-01
3c - Security Configuration Toolset	High	Beta Testing	Dec-00
3d - File Security Settings	High	Beta Testing	Dec-00
3e - Registry Security Settings	High	Beta Testing	Dec-00
3f - Local Policy Settings	High	Beta Testing	Dec-00
3g - Security Options	High	Beta Testing	Mar-01
3h - Restricted Groups	High	Beta Testing	Mar-01
3i - Event Log Settings	High	Beta Testing	Dec-00
3j - Account Policy	High	Beta Testing	Dec-00
3k - Administrative Templates	Med	Beta Testing	Mar-01
3l - .inf Configuration Templates	High	Beta Testing	Dec-00
4 - Non Windows 2000 Client Configuration	Ongoing		First Release Mar 01
4a - Windows 9x, NT4	Med	Beta Testing	Mar-01
4b - Unix Interoperability	Med	Draft	Apr-01
4c - Novell File Server (UFS)	Med	Outside	UFS Requirement
4d - SQL Apps (DISA)	Med	Outside/Review	DISA Requirement
5 - NT to Win 2000 Migration	High	Draft	May-01
5a - Mixed-Mode	Med		May-01
6 - DNS Configuration Guide	High	Beta Testing	Dec-00
7 - Encrypted File System	Low	Beta Testing	Mar-01
8 - File Resources (DISA)	Med	Beta Testing	Mar-01
9 - Other Network Services	Med	Ongoing	First Release Feb 01
9a - IPSec	Med	Draft	Apr-01
9b - Kerberos	Med	Class review	Apr-01
9c - Terminal Services (V2)	Med	Draft	Apr-01
9d - RAS	Med		Apr-01
9e - DHCP	Low	Beta Testing	Jan-01
9f - WINS	Low	Draft	Apr-01
10 - Router	Med	Draft	Apr-01
11 - ISA Server 2000 Guide	Med	Beta Testing	Mar-01
12 - Certificate Services	Med	Draft	Apr-01
12a - Windows 2000 Certificate Server	Med	Beta Testing	Feb-01
12b - Client Configuration	High	Beta Testing	Feb-01
12c - Non-Windows 2000 Certificate Server Integration	Low	On-going	Mar-01
12d - DoD PKI Certificates in Outlook 2000	Med	Class review	Apr-01
13 - Exchange 2000	Low	Draft	Jun-01
14 - Internet Information Server 5	Med	Beta Testing	Feb-01
15 - Secure S/W Installation	Low		Future
Group Policy Reference	Low	Beta testing	Dec-00
Value-added Tools	Med/Low	Ongoing	First Release Feb 01
Appendices - Supporting Documents			
A - Guide to Secure Config and Admin of IPlanet Web Server	Low	Beta Testing	Feb-01
B - Router (generic)	Med	Beta Testing	Dec-00
C - Office 97/Executable Content Security Risk and Countermeasures	Low	Beta Testing	Feb-01
D - VPN Guide	Low		Apr-01
E - Defense in-Depth White Paper	Low	Complete	Mar-01



UNCLASSIFIED D